

Ref-2

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-038445

(43)Date of publication of application : 05.02.2004

(51)Int.Cl.

G06K 19/10

B42D 15/10

G06K 17/00

G06K 19/073

H04L 9/08

H04L 9/10

H04L 9/32

(21)Application number : 2002-193162

(71)Applicant : NEC TOKIN CORP

(22)Date of filing : 02.07.2002

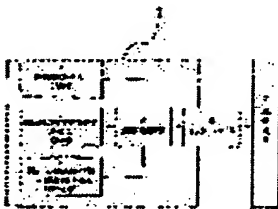
(72)Inventor : ARAI ATSUSHI

(54) IC CARD AND ENCRYPTION METHOD FOR THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain an IC card for transmitting a telegram with high confidentiality and integrity by performing secure messaging using a key of a public key encryption system.

SOLUTION: In an IC card and a higher-order device with a read only nonvolatile memory and a readable/writable nonvolatile memory, when the IC card transfers the telegram to the higher-order device, the IC card recognizes the confidentiality and integrity of the telegram by using two sets of paired public keys and secret keys.



Ref-2

対応なし、英抄

(19) 日本国特許庁 (JP) (12) 公開特許公報 (A) (11) 特許出願公開番号
特開2004-38445
(P2004-38445A)
(43) 公開日 平成16年2月5日 (2004. 2. 5)

(51) Int. Cl. ⁷	F I	テーマコード (参考)
G06K 19/10	G06K 19/00 R	2C005
B42D 15/10	B42D 15/10 521	5B035
G06K 17/00	G06K 17/00 S	5B058
G06K 19/073	G06K 19/00 P	5J104
H04L 9/08	H04L 9/00 621A	

審査請求 有 請求項の数 14 O L (全 9 頁) 最終頁に続く

(21) 出願番号	特願2002-193162 (P2002-193162)	(71) 出願人	000134257
(22) 出願日	平成14年7月2日 (2002. 7. 2)		NECトーキン株式会社
			宮城県仙台市太白区郡山6丁目7番1号
		(72) 発明者	荒井 篤志
			宮城県仙台市太白区郡山六丁目7番1号
			エヌイーシートーキン株式会社内
		Fターム (参考)	2C005 MA01 SA02 SA23
			5B035 AA13 BB09 CA38
			5B058 CA01 KA31 KA35
			5J104 AA16 EA04 EA15 NA02 NA12
			NA35

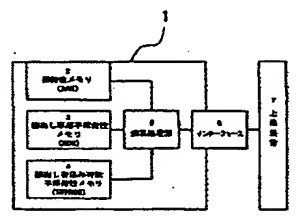
(54) 【発明の名称】 ICカードおよびICカードの暗号方法

(57) 【要約】

【課題】 公開鍵暗号方式の鍵を使用したセキュアメッセージングを行うことにより、隠蔽性、完全性の高い電文を送信することができるICカードを得る。

【解決手段】 少なくとも演算処理部、揮発性メモリ、読み出し専用不揮発性メモリ及び読み出し書き込み可能な不揮発性メモリを具備したICカード及び上位装置において、上位装置との電文の伝送において、対となっている公開鍵及び秘密鍵を2組使用して、前記電文の隠蔽及び完全性の確認を行うICカードとする。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

少なくとも演算処理部、揮発性メモリ、読み出し専用不揮発性メモリ及び読み出し書き込み可能な不揮発性メモリを具備した IC カード及び上位装置において、上位装置との電文の伝送において、対となっている公開鍵及び秘密鍵を 2 組使用して、前記電文の隠蔽及び完全性の確認を行うことを特徴とする IC カード。

【請求項 2】

前記 IC カードが保持している公開鍵対の公開鍵を上位装置が持ち、前記上位装置が保持している公開鍵対の公開鍵を前記 IC カードが持ち、前記 2 つの公開鍵対を伝送する電文の隠蔽及び完全性の確認に使用することを特徴とする請求項 1 に記載の IC カード。

10

【請求項 3】

前記 IC カードが起動後に前記 IC カードの持つ公開鍵対の公開鍵を上位装置に渡し、前記上位装置が起動後に前記上位装置の持つ公開鍵対の公開鍵を前記 IC カードに渡し、前記 2 つの公開鍵対を伝送する電文の隠蔽及び完全性の確認に使用することを特徴とする請求項 1 または 2 に記載の IC カード。

【請求項 4】

前記上位装置へ隠蔽及び完全性確認を行った電文を IC カードが送信する際に、前記上位装置が持つ公開鍵対の公開鍵を用いて平文を暗号化することで隠蔽を行い、前記 IC カードが持つ公開鍵対の秘密鍵を用いて、完全性確認のための認証子の暗号化を行うことで完全性の確認を行うことを特徴とする請求項 1 ないし 3 のいずれかに記載の IC カード。

20

【請求項 5】

前記上位装置から隠蔽及び完全性確認を行った電文を IC カードが受信した際に、前記上位装置が持つ公開鍵対の公開鍵を用いて、完全性確認のための認証子の復号化を行うことで完全性の確認を行い、前記 IC カードが持つ公開鍵対の秘密鍵を用いて、隠蔽された暗号文を復号化することを特徴とする請求項 1 ないし 3 のいずれかに記載の IC カード。

【請求項 6】

前記 IC カードの動作終了時に前記 IC カードが上位装置から受け取り、電文の隠蔽且つ完全性確認に使用した公開鍵を廃棄することを特徴とする請求項 1 ないし 5 のいずれかに記載の IC カード。

【請求項 7】

前記 IC カード起動後に前記 IC カードが、前記 IC カード内で作製した乱数により上位装置に渡す公開鍵を含む公開鍵対を新たに作製することを特徴とする請求項 1 ないし 5 のいずれかに記載の IC カード。

30

【請求項 8】

前記 IC カードが持つ電文の隠蔽且つ完全性の確認に使用する公開鍵対が読み出し専用不揮発性メモリに格納されていることを特徴とする請求項 1 ないし 5 のいずれかに記載の IC カード。

【請求項 9】

前記 IC カード起動後に交換される上位装置の公開鍵が揮発性メモリに格納されることを特徴とする請求項 1 ないし 8 のいずれかに記載の IC カード。

40

【請求項 10】

前記 IC カード起動後に交換される上位装置の公開鍵が、読み出し書き込み可能な不揮発性メモリに格納されることを特徴とする請求項 1 ないし 8 のいずれかに記載の IC カード。

【請求項 11】

前記 IC カード起動後に交換される上位装置の公開鍵を前記 IC カードの動作終了時まで使用することを特徴とする請求項 9 または 10 に記載の IC カード。

【請求項 12】

少なくとも演算処理部、揮発性メモリ、読み出し専用不揮発性メモリ及び読み出し書き込み可能な不揮発性メモリを具備した IC カードの認証方法において、IC カードと上位装

50

置との電文の伝送において、対となっている公開鍵及び秘密鍵を2組使用して、前記電文の隠蔽及び完全性の確認を行うことを特徴とするICカードの暗号方法。

【請求項13】

前記ICカードの暗号方法は、ICカードがセキュア電文を送信し、上位装置がセキュア電文を受信する場合に、上位装置は対となる第1の秘密鍵10と第1の公開鍵11を有し、前記ICカードは、前記上位装置より前記第1の公開鍵を取得し、前記ICカードは、取得した第1の公開鍵を、ICカード内のRAMまたはEEPROMに格納し、前記ICカードは、そのカード内部に、対となる第2の秘密鍵、第2の公開鍵を生成し、ついで、前記ICカードは第2の公開鍵を前記上位装置へ送信し、前記ICカードは、第1の公開鍵を使用して、上位装置に送信する平文を暗号化し暗号文を作成し、前記ICカードは、前記暗号文よりハッシュ値を作成し、前記ICカードは、前記ハッシュ値と第2の秘密鍵よりメッセージ認証子を作成し、前記ICカードは、メッセージ認証子を添付した暗号文を、上位装置に対して送信し、前記メッセージ認証子を添付した暗号文を受信した上位装置は、暗号文からハッシュ値を作成し、前記上位装置は、メッセージ認証子を第2の公開鍵を用いて復号化し、前記上位装置は、復号化したハッシュ値と、作成したハッシュ値を比較し、前記上位装置は、暗号文を第1の秘密鍵を使用して復号化し、ICカードより送信された平文を取り出すことを特徴とする請求項12に記載のICカードの暗号方法。

10

【請求項14】

前記ICカードの暗号方法は、上位装置がセキュア電文を送信し、ICカードがセキュア電文を受信する場合に、上位装置は対となる第1の秘密鍵10と第1の公開鍵11を有し、前記ICカードは、前記上位装置より前記第1の公開鍵を取得し、前記ICカードは、取得した第1の公開鍵を、ICカード内のRAMまたはEEPROMに格納し、前記ICカードは、そのカード内部に、対となる第2の秘密鍵、第2の公開鍵を生成し、ついで、前記ICカードは第2の公開鍵を前記上位装置へ送信し、上位装置は、第2の公開鍵を使用してICカードに送信する平文を暗号化し、暗号文を作成し、前記上位装置は、前記暗号文よりハッシュ値を作成し、前記上位装置は、前記ハッシュ値と第1の秘密鍵より、メッセージ認証子を作成し、上位装置は、前記メッセージ認証子を添付した暗号文をICカードに対して送信し、前記メッセージ認証子を添付した暗号文を受信した、ICカードは、暗号文からハッシュ値を作成し、前記ICカードは、前記メッセージ認証子を第1の公開鍵を用いて復号化し、ICカードは、前記復号化したハッシュ値と、作成したハッシュ値を比較し、ICカードは、暗号文を第2の秘密鍵を使用して復号化し、ICカードより送信された平文を取り出すことを特徴とする請求項12に記載のICカードの暗号方法。

20

30

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、主としてICカード及びその周辺装置との通信に際し、より秘密性の高い隠蔽及び完全性の確認を行うのに好適なICカードおよびICカードの暗号方法に関する。

【0002】

【従来の技術】

ICカードの通信と上位装置で通信する電文の隠蔽及び完全性確認（以後、セキュアメッセージングという）を行う場合には、一般的には共通鍵暗号方式の鍵が使用されていた。

40

【0003】

【発明が解決しようとする課題】

しかし、従来の共通鍵暗号方式では、ICカード側と、上位装置側とで共通鍵を使用していたために、以下の問題点があった。即ち、共通鍵を使用しているため、第三者が故意に共通鍵を盗んで使用すれば、暗号は解読されてしまう。従って、従来の共通鍵圧電方式は、秘密保持の点でセキュリティが不十分であり、隠蔽性が劣るものであった。

【0004】

従って、本発明の目的は、公開鍵暗号方式の鍵を使用したセキュアメッセージングを行うことにより、隠蔽性、完全性の高い電文を送信することができるICカードおよびICカ

50

ードの暗号方法を提供することである。

【0005】

【課題を解決するための手段】

本発明のＩＣカードは、少なくとも演算処理部、揮発性メモリ、読み出し専用不揮発性メモリ及び読み出し書き込み可能な不揮発性メモリを具備したＩＣカード及び上位装置において、上位装置との電文の伝送において、以後、公開鍵対を２組使用して、前記電文の隠蔽及び完全性の確認を行う機能を有するＩＣカードである。

【0006】

更に、本発明のＩＣカードは、ＩＣカードが保持している公開鍵対の公開鍵を上位装置が持ち、前記上位装置が保持している公開鍵対の公開鍵を前記ＩＣカードが持ち、前記２つの公開鍵対を伝送する電文の隠蔽及び完全性の確認に使用する機能を有するＩＣカードである。

【0007】

また、使用する公開鍵対を前記ＩＣカードが起動後にＩＣカードの持つ公開鍵対の公開鍵を上位装置に渡し、前記上位装置が起動後に上位装置の持つ公開鍵対の公開鍵をＩＣカードに渡し、前記２つの公開鍵対を伝送する電文の隠蔽及び完全性の確認に使用する機能を有するＩＣカードである。

【0008】

更に、本発明のＩＣカードは、上位装置へ隠蔽及び完全性確認を行った電文を送信する際に、前記上位装置が持つ公開鍵対の公開鍵を用いて平文を暗号化することで隠蔽を行い、前記ＩＣカードが持つ公開鍵対の秘密鍵を用いて、完全性確認のための認証子の暗号化を行うことで完全性の確認を行う機能を有するＩＣカードである。

【0009】

続いて、上位装置から隠蔽及び完全性確認を行った電文を受信した際に、前記上位装置が持つ公開鍵対の公開鍵を用いて、完全性確認のための認証子の復号化を行うことで完全性の確認を行い、前記ＩＣカードが持つ公開鍵対の秘密鍵を用いて、隠蔽された暗号文を復号化することを行う機能を有するＩＣカードである。

【0010】

更に、本発明のＩＣカードは、上位装置から受け取った公開鍵をＩＣカードの動作終了時に使用した前記公開鍵が廃棄される機能を有するＩＣカードである。

【0011】

更に、上位装置に渡す公開鍵を含む公開鍵対をＩＣカード起動後にＩＣカード内で作成した乱数により新たに作成する機能を有するＩＣカードである。

【0012】

更に、本発明のＩＣカードは、電文の隠蔽且つ完全性の確認に使用する前記ＩＣカードが持つ公開鍵対が読み出し専用不揮発性メモリに格納する機能を有するＩＣカードである。

【0013】

または、ＩＣカード起動後に交換される前記上位装置の公開鍵が揮発性メモリに格納される機能を有するＩＣカードである。

【0014】

または、ＩＣカード起動後に交換される前記上位装置の公開鍵が読み出し書き込み可能な不揮発性メモリに格納される機能を有するＩＣカードである。

【0015】

また、本発明は、少なくとも演算処理部、揮発性メモリ、読み出し専用不揮発性メモリ及び読み出し書き込み可能な不揮発性メモリを具備したＩＣカードの認証方法において、ＩＣカードと上位装置との電文の伝送において、対となっている公開鍵及び秘密鍵を２組使用して、前記電文の隠蔽及び完全性の確認を行うＩＣカードの暗号方法である。

【0016】

また、本発明は、前記ＩＣカードの暗号方法は、ＩＣカードがセキュア電文を送信し、上位装置がセキュア電文を受信する場合に、上位装置は対となる第１の秘密鍵１０と第１の

公開鍵 11 を有し、前記 IC カードは、前記上位装置より前記第 1 の公開鍵を取得し、前記 IC カードは、取得した第 1 の公開鍵を、IC カード内の RAM または EEPROM に格納し、前記 IC カードは、そのカード内部に、対となる第 2 の秘密鍵、第 2 の公開鍵を生成し、ついで、前記 IC カードは第 2 の公開鍵を前記上位装置へ送信し、前記 IC カードは、第 1 の公開鍵を使用して、上位装置に送信する平文を暗号化し暗号文を作成し、前記 IC カードは、前記暗号文よりハッシュ値を作成し、前記 IC カードは、前記ハッシュ値と第 2 の秘密鍵よりメッセージ認証子を作成し、前記 IC カードは、メッセージ認証子を添付した暗号文を、上位装置に対して送信し、前記メッセージ認証子を添付した暗号文を受信した上位装置は、暗号文からハッシュ値を作成し、前記上位装置は、メッセージ認証子を第 2 の公開鍵を用いて復号化し、前記上位装置は、復号化したハッシュ値と、作成したハッシュ値を比較し、前記上位装置は、暗号文を第 1 の秘密鍵を使用して復号化し、IC カードより送信された平文を取り出す IC カードの暗号方法である。 10

【0017】

また、本発明は、上位装置がセキュア電文を送信し、IC カードがセキュア電文を受信する場合に、前記 IC カードの暗号方法は、上位装置は対となる第 1 の秘密鍵 10 と第 1 の公開鍵 11 を有し、前記 IC カードは、前記上位装置より前記第 1 の公開鍵を取得し、前記 IC カードは、取得した第 1 の公開鍵を、IC カード内の RAM または EEPROM に格納し、前記 IC カードは、そのカード内部に、対となる第 2 の秘密鍵、第 2 の公開鍵を生成し、ついで、前記 IC カードは第 2 の公開鍵を前記上位装置へ送信し、上位装置は、第 2 の公開鍵を使用して IC カードに送信する平文を暗号化し、暗号文を作成し、前記上位装置は、前記暗号文よりハッシュ値を作成し、前記上位装置は、前記ハッシュ値と第 1 20 の秘密鍵より、メッセージ認証子を作成し、上位装置は、前記メッセージ認証子を添付した暗号文を IC カードに対して送信し、前記メッセージ認証子を添付した暗号文を受信した、IC カードは、暗号文からハッシュ値を作成し、前記 IC カードは、前記メッセージ認証子を第 1 の公開鍵を用いて復号化し、IC カードは、前記復号化したハッシュ値と、作成したハッシュ値を比較し、IC カードは、暗号文を第 2 の秘密鍵を使用して復号化し、IC カードより送信された平文を取り出す IC カードの暗号方法である。

【0018】

【発明の実施の形態】

以下、本発明の実施の形態による IC カードおよび IC カードの暗号方法について、IC カード本体および IC カードがセキュアメッセージング処理された電文（以後、セキュア電文という）を送信する場合と IC カードがセキュア電文を受信する場合とに分けて図面を用いて詳細に説明する。 30

【0019】

（実施の形態 1）

図 1 は、本発明の実施の形態 1 による IC カードの構成例を示したものである。本実施の形態の IC カード 1 内に搭載された IC チップ上には、上位装置 7 とデータ交換を行うインタフェース 6 と制御プログラムを処理する演算処理部 5 と、揮発性メモリ（RAM）2 と、制御プログラムを格納しておく読み出し専用不揮発性メモリ（ROM）3 と、書き込みまたは書き換えデータを格納する読み出し書き込み可能不揮発性メモリ（EEPROM）4 が具備されている。 40

【0020】

（実施の形態 2）

図 2 は、本発明の実施の形態 2 による IC カードの暗号方法の模式図であり、IC カード 9 がセキュア電文を送信し、上位装置 8 がセキュア電文を受信する場合の模式図である。

（1）上位装置 8 は対となる秘密鍵 10 と公開鍵 11 を持っている。

（2）IC カード 9 は上位装置 8 より公開鍵 11 を取得する。

（3）IC カード 9 は、取得した公開鍵 11 を揮発性メモリ 2 または読み出し書き込み可能不揮発性メモリ 4 に格納する。

（4）IC カード 9 は、そのカード内部に対となる秘密鍵 12、公開鍵 13 を生成する又 50

は持っている。

(5) ICカード9は公開鍵13を上位装置へ送信する。

(6) ICカード9は公開鍵11を使用して上位装置に送信する平文14を暗号化し暗号文15を作成する。

(7) ICカード9は暗号文15よりハッシュ値16を作成する。

(8) ICカード9はハッシュ値16と秘密鍵12よりメッセージ認証子17を作成する。

(9) ICカード9はメッセージ認証子17を添付した暗号文15を上位装置8に対して送信する。

(10) メッセージ認証子17を添付した暗号文15を受信した上位装置8は暗号文16からハッシュ値18を作成する。

(11) 上位装置8はメッセージ認証子17を公開鍵13を用いて復号化する。

(12) 上位装置8は復号化したハッシュ値19と作成したハッシュ値18を比較する。

(13) 上位装置8は暗号文15を秘密鍵10を使用して復号化し、ICカードより送信された平文20を取り出す。

【0021】

(実施の形態3)

図3は、本発明の実施の形態3によるICカードの暗号方法の模式図であり、上位装置8がセキュア電文を送信し、ICカード9がセキュア電文を受信する場合の模式図である。

(1) 上位装置8とICカード9が公開鍵を交換していない場合には、先の実施の形態2の(1)～(3)を行う。

(2) 上位装置8は公開鍵13を使用してICカード9に送信する平文21を暗号化し暗号文22を作成する。

(3) 上位装置8は暗号文22よりハッシュ値23を作成する。

(4) 上位装置8はハッシュ値23と秘密鍵10よりメッセージ認証子24を作成する。

(5) 上位装置8はメッセージ認証子24を添付した暗号文22をICカード9に対して送信する。

(6) メッセージ認証子24を添付した暗号文22を受信したICカード9は暗号文22からハッシュ値25を作成する。

(7) ICカード9はメッセージ認証子24を公開鍵11を用いて復号化する。

(8) ICカード9は復号化したハッシュ値26と作成したハッシュ値25を比較する。

(9) ICカード9は暗号文22を秘密鍵12を使用して復号化し、ICカードより送信された平文27を取り出す。

【0022】

通信終了後はICカード9内にある公開鍵11、秘密鍵12及び公開鍵13を廃棄し、次回起動時には新しい鍵を上位装置とICカード9で生成し交換することにより、より高い不正解読防止かつ書き換え防止機能となる。

【0023】

【発明の効果】

以上、本発明によれば、公開鍵暗号方式の鍵を使用したセキュアメッセージングを行うことにより、隠蔽性、完全性の高い電文を送信するセキュアメッセージングの方法を用いるICカードおよびICカード暗号方法を提供できる。これによって、ICカードと上位装置間の通信において、より不正解読、かつ不正書き換えが困難な通信が可能となる。

【図面の簡単な説明】

【図1】本発明の実施の形態1によるICカードの構成図。

【図2】本発明の実施の形態2によるICカードの暗号方法の模式図、ICカードがセキュア電文を送信し、上位装置がセキュア電文を受信する場合の模式図。

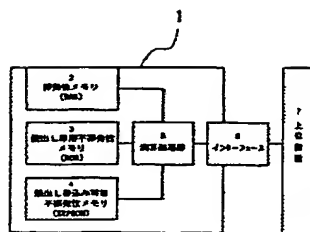
【図3】本発明の実施の形態3によるICカードの暗号方法の模式図、上位装置がセキュア電文を送信し、ICカードがセキュア電文を受信する場合の模式図。

【符号の説明】

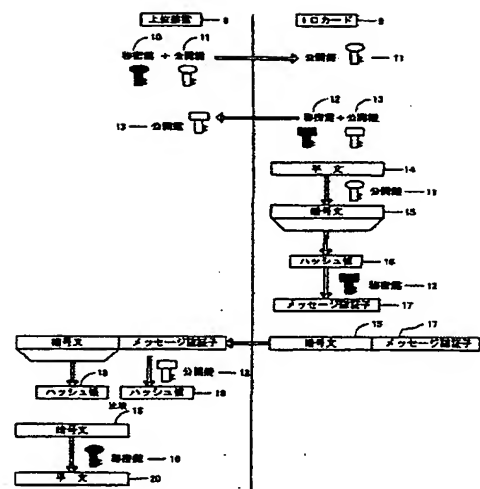
- 1, 9 ICカード
- 2 揮発性メモリ
- 3 読み出し専用不揮発性メモリ
- 4 読み出し書き込み可能専用不揮発性メモリ
- 5 演算処理部
- 6 インターフェース
- 7, 8 上位装置
- 10, 12 秘密鍵
- 11, 13 公開鍵
- 14, 20, 21, 27 平文
- 15, 22 暗号文
- 16, 18, 19, 23, 25, 26 ハッシュ値
- 17, 24 メッセージ認証子

10

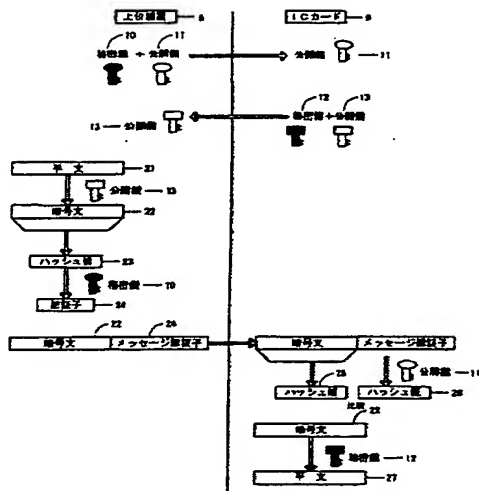
【図1】



【図2】



【図 3】



フロントページの続き

(51) Int. Cl. ⁷

F I

テーマコード (参考)

H 0 4 L 9/10

H 0 4 L 9/00 6 0 1 F

H 0 4 L 9/32

H 0 4 L 9/00 6 7 5 B